H.R. 5777

BEST PRACTICES Act (Introduced in House - IH)

HR 5777 IH

111th CONGRESS
2d Session
H. R. 5777

To foster transparency about the commercial use of personal information, provide consumers with meaningful choice about the collection, use, and disclosure of such information, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

July 19, 2010

Mr. RUSH introduced the following bill; which was referred to the Committee on Energy and Commerce

---

A BILL

To foster transparency about the commercial use of personal information, provide consumers with meaningful choice about the collection, use, and disclosure of such information, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) Short Title- This Act may be cited as the `Building Effective Strategies To Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards Act' or the `BEST PRACTICES Act'.
(b) Table of Contents- The table of contents for this Act is as follows:

TITLE I--TRANSPARENCY, NOTICE, AND INDIVIDUAL CHOICE

TITLE II--ACCURACY, ACCESS, AND DISPUTE RESOLUTION

TITLE III--DATA SECURITY, DATA MINIMIZATION, AND ACCOUNTABILITY

TITLE IV--SAFE HARBOR AND SELF-REGULATORY CHOICE PROGRAM

TITLE V--EXEMPTIONS

TITLE VI--APPLICATION AND ENFORCEMENT

TITLE VII--MISCELLANEOUS PROVISIONS

SEC. 2. DEFINITIONS.

As used in this Act, the following definitions apply:

(1) AGGREGATE INFORMATION- The term `aggregate information' means data that relates to a group or category of services or individuals, from which all information identifying an individual has been removed.

(2) COMMISSION- The term `Commission' means the Federal Trade Commission.

(3) COVERED ENTITY- The term `covered entity' means a person engaged in interstate commerce that collects or stores data containing covered information or sensitive information. Such term does not include--

(A) the Federal Government or any instrumentality of the Federal Government, nor the government of any State or political subdivision of a State; or

(B) any person that can demonstrate that such person--

(i) stores covered information from or about fewer than 15,000 individuals;

(ii) collects covered information from or about fewer than 10,000 individuals during any 12-month period;

(iii) does not collect or store sensitive information; and

(iv) does not use covered information to study, monitor, or analyze the behavior of individuals as the person's primary business.

(4) COVERED INFORMATION-

(A) IN GENERAL- The term `covered information' means, with respect to an individual, any of the following:

(i) the first name or initial and last name;

(ii) a postal address;

(iii) an email address;

(iv) a telephone or fax number;

(v) a tax identification number, passport number, driver's license number, or any other unique government-issued identification number;

(vi) a financial account number, or credit card or debit card number, or any required security code, access code, or password that is necessary to permit access to an individual's financial account;

(vii) any unique persistent identifier, such as a customer number, unique pseudonym or user alias, IP address, or other unique identifier, where such identifier is used to collect, store or identify information about a specific individual or to create or maintain a preference profile; or

(viii) any other information that is collected, stored, used, or disclosed in connection with any covered information described in clauses (i) through (vii).

(B) EXCLUSION- Such term shall not include--

(i) the title, business address, business email address, business telephone number, or business fax number associated with an individual's status as an employee of an organization, or an individual's name when collected, stored, used, or disclosed in connection with such employment status; or

(ii) any information collected from or about an employee by an employer, prospective employer, or former employer that directly relates to the employee-employer relationship.

(5) OPERATIONAL PURPOSE-

(A) IN GENERAL- The term `operational purpose' means a purpose reasonably necessary to facilitate, improve, or safeguard the logistical or technical ability of a covered entity to provide goods or services, manage its operations, comply with legal obligations, or protect against risks and threats, including--

(i) providing, operating, or improving a product or service used, requested, or authorized by an individual, including the ongoing provision of customer service and support;

(ii) analyzing data related to use of the product or service for purposes of improving the covered entity's products, services, or operations;

(iii) basic business functions such as accounting, inventory and supply chain management, quality assurance, and internal auditing;

(iv) protecting or defending the rights or property, including intellectual property, of the covered entity against actual or potential security threats, fraud, theft, unauthorized transactions, or other illegal activities;

(v) preventing imminent danger to the personal safety of an individual or group of individuals;

(vi) complying with a Federal, State, or local law, rule, or other applicable legal requirement, including disclosures pursuant to a court order, subpoena, summons, or other properly executed compulsory process; and

(vii) any other category of operational use specified by the Commission by regulation that is consistent with the purposes of this Act.

(B) EXCLUSION- Such term shall not include--

(i) the use of covered information for marketing or advertising purposes, or any use of or disclosure of covered information to a third party for such purposes; or

(ii) the use of covered information for a purpose that an individual acting reasonably under the circumstances would not expect based on the product or service used, requested, or authorized by the individual and, if known to the individual, would likely affect the individual's conduct or decisions with respect to the covered entity's products or services.

(6) PREFERENCE PROFILE- The term `preference profile' means a list of preferences, categories of information, or interests--

(A) associated with an individual or with an individual's computer or other device;

(B) inferred from the actual behavior of the individual, the actual use of the individual's computer or other device, or information supplied directly by the individual or other user of a computer or other device; and

(C) compiled and maintained for the purpose of marketing or purposes related to marketing, advertising, or sales.

(7) PUBLICLY AVAILABLE INFORMATION-

(A) IN GENERAL- The term `publicly available information' means any covered information or sensitive information that a covered entity has a reasonable basis to believe is lawfully made available to the general public from--

(i) Federal, State, or local government records;

(ii) widely distributed media; or

(iii) disclosures to the general public that are required to be made by Federal, State, or local law.

(B) CONSTRUCTION- A covered entity has a reasonable basis to believe that information is lawfully made available to the general public if the covered entity has taken steps to determine--

(i) that the information is of a type that is available to the general public; and

(ii) whether an individual can direct that the information not be made available to the general public and, if so, that the individual has not done so.

(8) SENSITIVE INFORMATION-

(A) DEFINITION- The term `sensitive information' means--

(i) any information that is associated with covered information of an individual and relates directly to that individual's--

(I) medical history, physical or mental health, or the provision of health care to the individual;

(II) race or ethnicity;

(III) religious beliefs and affiliation;

(IV) sexual orientation or sexual behavior;

(V) income, assets, liabilities, or financial records, and other financial information associated with a financial account, including balances and other financial information, except when financial account information is provided by the individual and is used only to process an authorized credit or debit to the account; or

(VI) precise geolocation information and any information about the individual's activities and relationships associated with such geolocation; or

(ii) an individual's--

(I) unique biometric data, including a fingerprint or retina scan; or

(II) Social Security number.

(B) MODIFIED DEFINITION BY RULEMAKING- The Commission may, by regulations promulgated under section 553 of title 5, United States Code, modify the scope or application of the definition of `sensitive information' for purposes of this Act. In promulgating such regulations, the Commission shall consider--

(i) the purposes of the collection of the information and the context of the use of the information;

(ii) how easily the information can be used to identify a specific individual;

(iii) the nature and extent of authorized access to the information;

(iv) an individual's reasonable expectations under the circumstances; and

(v) adverse effects that may be experienced by an individual if the information is disclosed to an unauthorized person.

(9) SERVICE PROVIDER- The term `service provider' means an entity that collects, maintains, processes, stores, or otherwise handles covered information or sensitive information on behalf of a covered entity, including, for the purposes of serving as a data processing center, distributing the information, providing customer support, maintaining the covered entity's records, information technology management, website or other hosting service, fraud detection, authentication, and other verification services, or performing other administrative support functions for the covered entity.

(10) THIRD PARTY-

(A) IN GENERAL- The term `third party' means, with respect to any covered entity, a person that--

(i) is not related to the covered entity by common ownership or corporate control; or

(ii) is a business unit or corporate entity that holds itself out to the public as separate from the covered entity, such that an individual acting reasonably under the circumstances would not expect it to be related to the covered entity or to have access to covered information the individual provides to that covered entity.

(B) COLLECTION OF INFORMATION BY MULTIPLE SOURCES- For the purpose of this definition, where multiple persons collect covered information or sensitive information from or about visitors to an online or mobile service, including a website, all such persons other than the operator or publisher of the online or mobile service or website shall be considered third parties unless--

(i) the person meets the requirements of the service provider exception in section 106(1); or

(ii) the person otherwise does not satisfy the requirements for a third party pursuant to the regulations implemented pursuant to subparagraph (C).

(C) RULEMAKING- Not later than 18 months after the date of the enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to clarify or modify the definition of third party for purposes of this Act. In promulgating such regulations, the Commission shall consider--

(i) the brand or brands associated with a covered entity;

(ii) the scope and nature of the businesses engaged in by a covered entity and a third party, including the nature of the products or services offered by the covered entity and third party; and

(iii) the relationship between a covered entity and a third party, taking into account such factors as ownership and control.

TITLE I--TRANSPARENCY, NOTICE, AND INDIVIDUAL CHOICE

SEC. 101. INFORMATION TO BE MADE AVAILABLE.

A covered entity shall, in accordance with the regulations issued under section 102, make available to individuals whose covered information or sensitive information it collects or maintains the following information about its information privacy practices and an individual's options with regard to such practices:

(1) The identity of the covered entity.

(2) A description of any covered information or sensitive information collected or stored by the covered entity.

(3) The specific purposes for which the covered entity collects and uses the covered information or sensitive information, including disclosure as to whether and how the covered entity customizes products or services or changes the prices of products or services based, in whole or in part, on covered information or sensitive information about individual customers or users.

(4) The specific purposes for which covered information or sensitive information may be disclosed to a third party and the categories of third parties who may receive such information for each such purpose.

(5) The choice and means the covered entity offers individuals for limiting the collection, use, and disclosure of covered information or sensitive information, in accordance with sections 103 and 104.

(6) A description of the information for which an individual may request access and the means to request such access, in accordance with section 202.

(7) How the covered entity may merge, link, or combine covered information or sensitive information collected from the individual with other information about the individual that the covered entity may acquire from third parties.

(8) The retention schedule for covered information and sensitive information in days, months, or years, or a statement that the covered entity will retain such information indefinitely or permanently.

(9) Whether or not an individual has the right to direct the covered entity to delete information collected from or about the individual.

(10) A reasonable means by which an individual may contact the covered entity with any inquiries or complaints regarding the covered entity's practices

concerning the collection, use, disclosure, or handling of the individual's covered information or sensitive information in accordance with section 302(a).
(11) The process by which the covered entity notifies individuals of material changes to its policies and practices.
(12) A hyperlink to or a listing of the Commission's online consumer complaint form or the toll-free number for the Commission's Consumer Response Center.
(13) The effective date of the privacy notice.

SEC. 102. PROVISION OF NOTICE OR NOTICES.

(a) In General- It shall be unlawful for a covered entity to collect, use, or disclose covered information or sensitive information unless it provides the information set forth in section 101 in concise, meaningful, timely, prominent, and easy-to-understand notice or notices, in accordance with the regulations issued by the Commission under subsection (b).
(b) Rulemaking- Not later than 18 months after the date of the enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to implement this section. In promulgating such regulations, the Commission--

(1) shall determine the means and timing of the notices required under this section, taking into account the different media, devices, or methods through which the covered entity collects covered information or sensitive information;
(2) shall have the authority to allow for, or require, the provision of short notices or limited disclosures that do not include all of the information set forth in section 101, if the Commission by regulation--

(A) requires the information to be otherwise clearly and conspicuously disclosed or available to individuals; and
(B) determines that the provision of such short notices or limited disclosures will accomplish the purposes of this Act to enhance transparency and provide individuals with meaningful choice regarding the collection, use, and disclosure of their covered information or sensitive information;

(3) shall consider--

(A) whether the notice or notices provide individuals with timely, effective, and meaningful notice that will enable an individual to understand relevant information and make informed choices;
(B) whether providing notice to individuals prior to or contemporaneously with the collection of covered information is practical or reasonable under the circumstances;
(C) the costs of implementing the prescribed notice or notices;
(D) the different media and context through which covered information is collected;
(E) whether it is reasonable and appropriate under the circumstances for a third party or a service provider to be responsible for providing notice and obtaining consent as required by this title in lieu of a covered entity; and
(F) the risk to consumers and commerce of over-notification; and

(4) may issue model notices.

(c) Exclusion From Notice Requirements-

(1) TRADE SECRET INFORMATION- Nothing in this section shall require a covered entity to reveal confidential, trade secret, or proprietary information.
(2) IN-PERSON TRANSACTIONS- Notice under this section shall not be required for in-person collection of covered information if--
(A) the covered information is collected for an operational purpose; or
(B) the covered entity only is collecting the name, address, email address, telephone or fax number of an individual and does not--
(i) share the covered information with third parties; or
(ii) use the covered information to acquire additional information about the individual from third parties.

(d) Retention- A covered entity shall retain copies of the notice or notices issued pursuant to this section for a period of 6 years after the date on which such notice was issued or the date when it was last in effect, whichever is later, unless the Commission determines pursuant to the rulemaking required under subsection (b) that such retention is not practical under the circumstances.

SEC. 103. OPT-OUT CONSENT REQUIRED FOR COLLECTION AND USE OF COVERED INFORMATION BY A COVERED ENTITY.

(a) In General- Except as provided in subsections (e) and (f) and section 106, it shall be unlawful for a covered entity to collect or use covered information about an individual without the consent of that individual, as set forth in this section. A covered entity shall be considered to have the consent of an individual for the collection and use of covered information about the individual if--
(1) the covered entity has provided to the individual notice required under section 102 and its implementing regulations;
(2) the covered entity provides the individual with a reasonable means to exercise an opt-out right and decline consent for such collection and use; and
(3) the individual either affirmatively grants consent for such collection and use or does not decline consent at the time notice is presented or made available to the individual.

(b) Duration of Individual's Opt-Out- An individual's direction to opt out under this section is effective permanently, unless otherwise directed by the individual.
(c) Subsequent Opt-Out- A covered entity shall provide an individual with a reasonable means to decline consent or revoke previously granted consent at any time.
(d) More Detailed Options- A covered entity may comply with this section by enabling an individual to decline consent for specific uses of his or her covered information, provided the individual has been given the opportunity to decline consent for the collection and use of covered information for all purposes, other than for an operational purpose excepted by subsection (e), for which covered information may be collected and used by the covered entity.
(e) Exception for Operational Purposes- This section shall not apply to the collection or use of covered information for an operational purpose.
(f) Collection and Use as a Condition of Service- Nothing in this section shall prohibit a covered entity from requiring, as a condition of an individual's receipt of a service or other benefit, including the receipt of an enhanced or premium version of a product or

service otherwise available, the reasonable collection and use of covered information about the individual, provided that--

(1) the covered entity has a direct relationship with the individual;

(2) the covered information is not shared with any third party except with the express affirmative consent as set forth in section 104;

(3) the covered entity provides a clear, prominent, and specific statement describing the specific purpose or purposes for which covered information may be used pursuant to section 101;

(4) the individual provides consent by acknowledging the specific uses set forth in the clear and prominent statement required under paragraph (3) as part of receiving the service or other benefit from the covered entity; and

(5) the individual is able to later withdraw consent for the use by canceling the service or otherwise indicating that he or she no longer wishes to receive the service or other benefit.

SEC. 104. EXPRESS AFFIRMATIVE CONSENT.

(a) Disclosure of Covered Information to Third Parties-

(1) DISCLOSURE PROHIBITED- Except as provided in section 106 and subject to title IV of this Act, it shall be unlawful for a covered entity to disclose covered information about an individual to a third party unless the covered entity has received express affirmative consent from the individual prior to the disclosure.

(2) EXCEPTION FOR JOINT MARKETING- Express affirmative consent shall not be required for any disclosure related to the performance of joint marketing, if the covered entity and the third party enter into a contractual agreement prohibiting the third party from disclosing or using the covered information except as necessary to carry out the joint marketing relationship.

(b) Collection, Use, or Disclosure of Sensitive Information- Except as provided in section 106, a covered entity may not collect, use, or disclose sensitive information from or about an individual for any purpose unless the covered entity obtains the express affirmative consent of the individual.

(c) Comprehensive Online Data Collection- A covered entity may not use hardware or software to monitor all or substantially all of the individual's Internet browsing or other significant class of Internet or computer activity and collect, use, or disclose information concerning such activity, except--

(1) with the express affirmative consent of the individual;

(2) for the purpose of making such information accessible to the individual or for use by the individual; or

(3) as provided in section 106.

(d) Limitation- A third party that receives covered information or sensitive information from a covered entity pursuant to this section shall only use such information for the specific purposes authorized by the individual when the individual granted express affirmative consent for the disclosure of the information to a third party.

(e) Revocation of Consent- A covered entity that has obtained the express affirmative consent of an individual pursuant to this section and section 105 shall provide the

individual with a reasonable means, without charge, to withdraw consent at any time thereafter.

SEC. 105. MATERIAL CHANGES TO PRIVACY PRACTICES.

(a) Retroactive Application- A covered entity shall provide the notice required by section 102 and obtain the express affirmative consent of the individual prior to making a material change in privacy practices governing previously collected covered information or sensitive information from that individual.

(b) Prospective Application- A covered entity shall not make material changes to its privacy practices governing the collection, use, or disclosure of covered information or sensitive information that has not been previously collected unless, 30 days before the effective date of the material change--

(1) the covered entity provides individuals with notice of the material change in accordance with section 102; and

(2) if required by sections 103 and 104, obtains the individual's consent to the material change or allows the individual to terminate the individual's relationship with the covered entity.

SEC. 106. EXCEPTIONS.

The consent requirements of sections 103 and 104 shall not apply to the following:

(1) SERVICE PROVIDERS-

(A) When a covered entity discloses covered information or sensitive information to a service provider performing services or functions on behalf of and under the instruction of the covered entity, provided--

(i) the covered entity obtained the required consent for the initial collection of such information and provided notice as required by section 102;

(ii) the covered entity enters into a contractual agreement that prohibits the service provider from using or disclosing the information other than to carry out the purposes for which the information was disclosed; and

(iii) in such cases, the covered entity remains responsible and liable for the protection of covered information and sensitive information that has been transferred to a service provider for processing.

(B) When a service provider subsequently discloses the information to another service provider in order to perform the same services or functions described in paragraph (1) on behalf of the covered entity.

(2) FRAUD DETECTION- Collection, use, or disclosure necessary to protect or defend the rights or property, including intellectual property, of the covered entity against actual or potential security threats, fraud, theft, unauthorized transactions, or other illegal activities.

(3) IMMINENT DANGER- Collection, use, or disclosure necessary to prevent imminent danger to the personal safety of an individual or group of individuals.

(4) COMPLIANCE WITH LAW- Collection, use, or disclosure required in order to comply with a Federal, State, or local law, rule, or other applicable legal requirement, including disclosures pursuant to subpoena, summons, or other properly executed compulsory process.
(5) PUBLICLY AVAILABLE INFORMATION- Collection, use, or disclosure of publicly available information, except that a covered entity may not use publicly available information about an individual for marketing purposes if the individual has opted out of the use by such covered entity of covered information or sensitive information for marketing purposes.

TITLE II--ACCURACY, ACCESS, AND DISPUTE RESOLUTION

SEC. 201. ACCURACY.

(a) Reasonable Procedures- Each covered entity shall establish reasonable procedures to assure the accuracy of the covered information or sensitive information it collects, assembles, or maintains. Not later than 18 months after the date of the enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to implement this section. In promulgating such regulations, the Commission shall consider--

(1) the costs and benefits of ensuring the accuracy of the information;
(2) the sensitivity of the information;
(3) the purposes for which the information will be used; and
(4) the harms from misuse of the information.

(b) Limited Exception for Fraud Databases- The requirement in subsection (a) shall not prevent the collection or maintenance of information that may be inaccurate with respect to a particular individual when that information is being collected or maintained solely--

(1) for the purpose of indicating whether there may be a discrepancy or irregularity in the covered information or sensitive information that is associated with an individual; and
(2) to help identify, or authenticate the identity of, an individual, or to protect against or investigate fraud or other unlawful conduct.

(c) Limited Exception for Publicly Available Information- Subject to section 202, a covered entity shall not be required to verify the accuracy of publicly available information if the covered entity has reasonable procedures to ensure that the publicly available information assembled or maintained by the covered entity accurately reflects the information available to the general public.

SEC. 202. ACCESS AND DISPUTE RESOLUTION.

(a) Access and Correction- A covered entity shall, upon request, provide an individual with reasonable access to, and the ability to dispute the accuracy or completeness of, covered information or sensitive information about that individual if such information may be used for purposes that could result in an adverse decision against the individual, including the denial of a right, benefit, or privilege.
(b) Access to Personal Profiles-

(1) IN GENERAL- Subject to title IV, a covered entity shall, upon request, provide an individual with reasonable access to any personal profile about that individual that the entity stores in a manner that makes it accessible in the normal course of business.

(2) SPECIAL RULE FOR PREFERENCE PROFILES- With respect to a preference profile, the obligation to provide access and correction under this section is met if the covered entity provides the ability to review and change the preference information associated with a unique persistent identifier.

(3) PARTICIPATION IN CHOICE PROGRAM- This subsection shall not apply to a covered entity that participates in a Choice Program under title IV.

(c) Notice in Lieu of Access- Subject to subsection (b), in those instances in which covered information or sensitive information is used only for purposes that could not reasonably result in an adverse decision against an individual, including the denial of a right, benefit, or privilege, a covered entity shall, upon request by an individual, provide the individual with a general notice or representative sample of the type or types of information the covered entity typically collects or stores for such purposes.

(d) Exceptions-

(1) A covered entity may decline to provide an individual with access to covered information or sensitive information if the covered entity reasonably believes--

(A) the individual requesting access cannot reasonably verify his or her identity as the person to which the information relates;

(B) access by the individual to the information is limited by law or legally recognized privilege;

(C) the information is used for a legitimate governmental or fraud prevention purpose that would be compromised by such access;

(D) such request for access is frivolous or vexatious;

(E) the privacy or other rights of persons other than the individual would be violated; or

(F) proprietary or confidential information, technology, or business processes would be revealed as a result.

(2) Where an exception described in paragraph (1) applies only to a portion of the covered information or sensitive information maintained by the covered entity, the covered entity shall provide access required under subsections (a) and (b) to the information to which the exception does not apply.

(3) A covered entity may decline an individual's request to correct or amend covered information or sensitive information pertaining to that individual where--

(A) a reason for denying access to the information under paragraph (1) would also apply to the request to correct or amend the information; or

(B) doing so would be incompatible with a legal obligation, such as a requirement to retain certain information.

(e) Fees- A covered entity may charge a reasonable fee, as determined by the Commission, for providing access in accordance with subsection (a) or (b).

(f) Time Limit- A covered entity shall respond to any access, correction, or amendment request within 30 days of the receipt of the request. Such response must consist of one or more of the following:

(1) The requested information in accordance with subsection (a) or (b).

(2) The general notice in accordance with subsection (c).
(3) Instructions for accessing, correcting, or amending the requested information through an automated mechanism.
(4) A confirmation that the requested corrections or amendments have been made.
(5) A notification that the covered entity is declining to correct or amend information pursuant to one of the exceptions described in subsection (d). Such notification shall include the reason or reasons for not making the suggested correction or amendment, unless one or more of such exceptions would also apply to the disclosure of the reason or reasons.
(6) A request to resubmit the access request and an explanation of why the original access request was deficient in cases where--
(A) the scope or nature of the request is unclear or the entity needs more information in order to respond to the request;
(B) the entity charges a fee as permitted under subsection (e), and the fee has not been paid; or
(C) the entity provides interested members of the public other reasonable and accessible instructions for submitting an access request and such instructions were not followed.
(7) A notification that additional time is needed where--
(A) the entity cannot reasonably provide a full response within 30 days of the receipt of the access; and
(B) the time extension needed for a full response is no greater than an additional 30 days.

(g) Rule of Construction- Nothing in this Act creates an obligation on a covered entity to provide an individual with the right to delete information.
(h) Additional Requirements Where Correction or Amendment Is Declined- If the covered entity declines to correct or amend the information described in subsection (a), the covered entity shall--
(1) note that the information is disputed, including the individual's statement disputing such information, and take reasonable steps to verify such information under the procedures outlined in section 201 if such information can be independently verified; and
(2) where the information was obtained from a third party or is publicly available information, inform the individual of the source of the information, and if reasonably available, where a request for correction may be directed, and, if the individual provides proof that the information is incorrect, correct the inaccuracy in the covered entity's records.

(i) Other Limitations- The obligations under this section do not, by themselves, create any obligation on the covered entity to retain, maintain, reorganize, or restructure covered information or sensitive information.
(j) Data Retention Exception- Covered information or sensitive information retained by the covered entity for under 30 days, or such other period of time as the Commission may determine, shall not be subject to this section.
(k) Rulemaking- Not later than 18 months after the date of the enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to implement this section. In addition, the Commission shall promulgate

regulations, as necessary, on the application of the exceptions and limitations in subsection (d), including any additional circumstances in which a covered entity may limit access to information under such subsection that the Commission determines to be appropriate.

TITLE III--DATA SECURITY, DATA MINIMIZATION, AND ACCOUNTABILITY

SEC. 301. DATA SECURITY.

(a) In General- Each covered entity and service provider shall establish, implement, and maintain reasonable and appropriate administrative, technical, and physical safeguards to--

(1) ensure the security, integrity, and confidentiality of the covered information or sensitive information it collects, assembles, or maintains;

(2) protect against any anticipated threats, reasonably foreseeable vulnerabilities, or hazards to the security or integrity of such information; and

(3) protect against unauthorized access to or use of such information and loss, misuse, alteration, or destruction of such information.

(b) Factors for Appropriate Safeguards- Not later than 18 months after the date of the enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to implement this section. In promulgating such regulations, the Commission shall consider--

(1) the size and complexity of an entity;

(2) the nature and scope of the activities of an entity;

(3) the sensitivity of the information;

(4) the current state of the art in administrative, technical, and physical safeguards for protecting information; and

(5) the cost of implementing such safeguards.

SEC. 302. ACCOUNTABILITY.

(a) Complaints to the Covered Entity- A covered entity shall provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this Act.

(b) Privacy Risk Assessment- A covered entity shall conduct an assessment of the risks to individuals raised by the collection, use, and disclosure of covered information or sensitive information prior to the implementation of commercial projects, marketing initiatives, business models, applications, and other products or services in which the covered entity intends to collect, or believes there is a reasonable likelihood it will collect, covered information or sensitive information from or about more than 1,000,000 individuals.

(c) Periodic Evaluation of Practices- A covered entity shall conduct periodic assessments to evaluate--

(1) whether the covered information or sensitive information the covered entity has collected is and remains necessary for the purposes disclosed at the time of collection pursuant to section 101 (c) and (d); and

(2) whether the covered entity's ongoing collection practices are and remain necessary for a legitimate business purpose.

SEC. 303. DATA MINIMIZATION OBLIGATIONS.

A covered entity that uses covered information or sensitive information for any purpose shall retain such data only as long as necessary to fulfill a legitimate business purpose or comply with a legal requirement.

TITLE IV--SAFE HARBOR AND SELF-REGULATORY CHOICE PROGRAM

SEC. 401. SAFE HARBOR.

A covered entity that participates in, and is in compliance with, 1 or more self-regulatory programs approved by the Commission under section 402 (in this title referred to as a `Choice Program') shall not be subject to--

(1) the requirements for express affirmative consent required under subsection 104(a) for the specified uses of covered information addressed by the Choice Program as described in section 403(1)(A);

(2) the requirement of access to information under section 202(b); or

(3) liability in a private right of action brought under section 604.

SEC. 402. APPROVAL BY THE FEDERAL TRADE COMMISSION.

(a) Initial Approval- Not later than 270 days after the submission of an application for approval of a Choice Program under this section, the Commission shall approve or decline to approve such program. The Commission shall only approve such program if the Commission finds, after notice and comment, that the program complies with the requirements of section 403.

(b) Approval of Modifications- The Commission shall approve or decline to approve any material change in a Choice Program previously approved by the Commission within 120 days after submission of an application for approval by such program. The Commission shall only approve such material change if the Commission finds, after notice and comment, that the proposed change complies with the requirements of section 403.

(c) Duration- A Choice Program approved by the Commission under this section shall be approved for a period of 5 years.

(d) Appeals- Final action by the Commission on a request for approval, or the failure to act within 270 days on a request for approval, submitted under this section may be appealed to a district court of the United States of appropriate jurisdiction as provided for in section 706 of title 5, United States Code.

SEC. 403. REQUIREMENTS OF SELF-REGULATORY PROGRAM.

To be approved as a Choice Program under this section, a program shall--

(1) provide individuals with--

(A) a clear and conspicuous opt-out mechanism that, when selected by the individual, prohibits all covered entities participating in the Choice Program from disclosing covered information to a third party for 1 or more specified uses, and may offer individuals a preference management tool that will enable an individual to make more detailed choices about the transfer of covered information to a third party; and

(B) a clear and conspicuous mechanism to set communication preferences, online behavioral advertising preferences, and such other preferences as the Choice Program may determine, subject to the approval of the Commission, that when selected by the individual, applies the individual's selected preferences to all covered entities participating in the Choice Program; and

(2) establish--

(A) guidelines and procedures requiring a participating covered entity to provide equivalent or greater protections for individuals and their covered information and sensitive information as are provided under titles I and II;

(B) procedures for reviewing applications by covered entities to participate in the Choice Program;

(C) procedures for periodic assessment of its procedures and for conducting periodic random compliance testing of covered entities participating in such Choice Program; and

(D) consequences for failure to comply with program requirements, such as public notice of the covered entity's noncompliance, suspension, or expulsion from the program, or referral to the Commission for enforcement.

SEC. 404. RULEMAKING.

Not later than 18 months after the date of enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to implement this section and to provide compliance guidance for entities seeking to be approved under this title, including regulations--

(1) establishing criteria for the submission of the application, including evidence of how the Choice Program will comply with the requirements of section 403;

(2) establishing criteria for opt-out mechanisms and communication preferences, online behavioral advertising preferences, or other preferences meeting the requirements of this title;

(3) establishing consequences for failure to comply with the requirements of section 403, such as public notice of the Choice Program's noncompliance and suspension or revocation of the Commission's approval of such Program as described in section 402;

(4) allowing for and promoting continued evolution and innovation in privacy protection, meaningful consumer control, simplified approaches to disclosure, and transparency; and

(5) providing additional incentives for self-regulation by covered entities to implement the protections afforded individuals under titles I and II of this Act,

including provisions for ensuring that a covered entity will be considered to be in compliance with the requirements of titles I and II and the regulations issued under such titles if that covered entity complies with guidelines or requirements of a Choice Program approved under section 402.

TITLE V--EXEMPTIONS

SEC. 501. USE OF AGGREGATE OR DEIDENTIFIED INFORMATION.

(a) General Exclusion- Subject to subsections (b) and (c), nothing in this Act shall preclude a covered entity from collecting, using, or disclosing--

(1) aggregate information; or

(2) covered information or sensitive information from which identifying information has been obscured or removed using reasonable and appropriate methods such that the remaining information does not identify, and there is no reasonable basis to believe that the information can be used to identify--

(A) the specific individual to whom such covered information relates; or

(B) a computer or device owned or used by a specific individual.

(b) Reasonable Procedures for Disclosure- If a covered entity discloses the information described in paragraphs (1) and (2) of subsection (a) to a third party, the covered entity shall take reasonable steps to protect such information, including, in the case of the information described in such paragraph (2), not disclosing the algorithm or other mechanism used to obscure or remove the identifying information, and obtaining satisfactory written assurance that the third party will not attempt to reconstruct the identifying information.

(c) Prohibition on Reconstructing or Revealing Identifying Information-

(1) IN GENERAL- It shall be unlawful for any person to reconstruct or reveal the identifying information that has been removed or obscured (as described in subsection (a)(2)) and for which a covered entity claims or has claimed the benefit of the general exemption in subsection (a).

(2) RULEMAKING- Not later than 18 months after the date of the enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to establish exemptions to this subsection. In promulgating such regulations, the Commission shall consider--

(A) the purposes for which such identifying information may need to be reconstructed or revealed;

(B) the size and sensitivity of the data set; and

(C) public policy issues such as health, safety, and national security.

SEC. 502. ACTIVITIES COVERED BY OTHER FEDERAL PRIVACY LAWS.

Except as provided expressly in this Act, this Act shall have no effect on activities covered by any of the following:

(1) Title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.).

(2) The Fair Credit Reporting Act (15 U.S.C. 1681 et seq.).

(3) The Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191).
(4) Part C of title XI of the Social Security Act (42 U.S.C. 1320d et seq.).
(5) Sections 222 and 631 of the Communications Act of 1934 (47 U.S.C. 222 and 47 U.S.C. 551).
(6) The Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq.).
(7) The CAN-SPAM Act of 2003 (15 U.S.C. 7701 et seq.).
(8) The Electronic Communications Privacy Act of 1986 (18 U.S.C. 2510 et seq.).
(9) The Video Privacy Protection Act (18 U.S.C. 2710 et seq.).

TITLE VI--APPLICATION AND ENFORCEMENT

SEC. 601. GENERAL APPLICATION.

The requirements of this Act shall only apply to those persons over which the Commission has authority pursuant to section 5(a)(2) of the Federal Trade Commission Act. Notwithstanding any provision of such Act or any other provision of law, common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.) and any amendment thereto shall be subject to the jurisdiction of the Commission for purposes of this Act.

SEC. 602. ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.

(a) Unfair or Deceptive Acts or Practices- A violation of titles I, II, or III shall be treated as an unfair and deceptive act or practice in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices.
(b) Powers of Commission- The Commission shall enforce this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act. Any person who violates this Act or the regulations issued under this Act shall be subject to the penalties and entitled to the privileges and immunities provided in that Act.
(c) Rulemaking Authority-

(1) RULEMAKING- The Commission may, in accordance with section 553 of title 5, United States Code, issue such regulations it determines to be necessary to carry out this Act.
(2) AUTHORITY TO GRANT EXCEPTIONS- The regulations prescribed under paragraph (1) may include such additional exceptions to titles I, II, III, IV, and V of this Act as the Commission considers consistent with the purposes of this Act.
(3) LIMITATION- In promulgating rules under this Act, the Commission shall not require the deployment or use of any specific products or technologies, including any specific computer software or hardware.

SEC. 603. ENFORCEMENT BY STATE ATTORNEYS GENERAL.

(a) Civil Action- In any case in which the Attorney General of a State, or an official or agency of a State, has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by any person who violates this Act, the attorney general, official, or agency of the State, as parens patriae, may bring a civil action on behalf of the residents of the State in an appropriate district court of the United States--

(1) to enjoin further violation of this Act by the defendant;

(2) to compel compliance with this Act; or

(3) for violations of titles I, II, or III of this Act, to obtain civil penalties in the amount determined under subsection (b).

(b) Civil Penalties-

(1) CALCULATION- For purposes of calculating the civil penalties that may be obtained under subsection (a)(3)--

(A) with regard to a violation of title I, the amount determined under this paragraph is the amount calculated by multiplying the number of days that a covered entity is not in compliance with such title, or the number of individuals for whom the covered entity failed to obtain consent as required by such title, whichever is greater, by an amount not to exceed $11,000; and

(B) with regard to a violation of title II or III, the amount determined under this paragraph is the amount calculated by multiplying the number of days that a covered entity is not in compliance with such title or titles by an amount not to exceed $11,000.

(2) ADJUSTMENT FOR INFLATION- Beginning on the date that the Consumer Price Index for All Urban Consumers is first published by the Bureau of Labor Statistics that is after 1 year after the date of enactment of this Act, and each year thereafter, the amounts specified in subparagraphs (A) and (B) of paragraph (1) shall be increased by the percentage increase in the Consumer Price Index published on that date from the Consumer Price Index published the previous year.

(3) MAXIMUM TOTAL LIABILITY- Notwithstanding the number of actions which may be brought against a person under this section the maximum civil penalty for which any person may be liable under this section shall not exceed--

(A) $5,000,000 for any related series of violations of title I; and

(B) $5,000,000 for any related series of violations of title II and title III.

(4) EFFECT OF PARTICIPATION IN CHOICE PROGRAM- If a covered entity participates in a Choice Program established under title IV and cures the alleged violation of title I or II in a reasonable period of time after receiving notice of the alleged violation, such conduct shall be taken into consideration by a State or a court in determining the amount of civil penalties under this subsection.

(c) Intervention by the FTC-

(1) NOTICE AND INTERVENTION- The State shall provide prior written notice of any action under subsection (a) to the Commission and provide the Commission with a copy of its complaint, except in any case in which such prior notice is not feasible, in which case the State shall serve such notice immediately upon instituting such action. The Commission shall have the right--

(A) to intervene in the action;
(B) upon so intervening, to be heard on all matters arising therein; and
(C) to file petitions for appeal.

(2) LIMITATION ON STATE ACTION WHILE FEDERAL ACTION IS PENDING- If the Commission has instituted a civil action for violation of this Act, no attorney general of a State, or official, or agency of a State, may bring an action under this section during the pendency of that action against any defendant named in the complaint of the Commission for any violation of this Act alleged in the complaint.

(d) Construction- For purposes of bringing any civil action under subsection (a), nothing in this Act shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to--

(1) conduct investigations;
(2) administer oaths or affirmations; or
(3) compel the attendance of witnesses or the production of documentary and other evidence.

SEC. 604. PRIVATE RIGHT OF ACTION.

(a) In General- A covered entity, other than a covered entity that participates in and is in compliance with a Choice Program established under title IV, who willfully fails to comply with sections 103 or 104 of this Act with respect to any individual is liable to that individual in a civil action brought in a district court of the United States of appropriate jurisdiction in an amount equal to the sum of--

(1) the greater of any actual damages of not less than $100 and not more than $1,000;
(2) such amount of punitive damages as the court may allow; and
(3) in the case of any successful action under this section, the costs of the action together with reasonable attorney's fees as determined by the court.

(b) Limitation- A civil action under this section may not be commenced later than 2 years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

SEC. 605. EFFECT ON OTHER LAWS.

(a) Preemption of State Laws- This Act supersedes any provision of a statute, regulation, or rule of a State or political subdivision of a State, with respect to those entities covered by the regulations issued pursuant to this Act, that expressly requires covered entities to implement requirements with respect to the collection, use, or disclosure of covered information addressed in this Act.

(b) Additional Preemption-

(1) IN GENERAL- No person other than a person specified in section 603 or 604 may bring a civil action under the laws of any State if such action is premised in whole or in part upon the defendant violating any provision of this Act.

(2) PROTECTION OF STATE CONSUMER PROTECTION LAWS- This subsection shall not be construed to limit the enforcement of any State consumer protection law by an attorney general or other official of a State.

(c) Protection of Certain State Laws- This Act shall not be construed to preempt the applicability of--

(1) State laws that address the collection, use, or disclosure of health information or financial information;

(2) State laws that address notification requirements in the event of a data breach;

(3) State trespass, contract, or tort law; or

(4) other State laws to the extent that those laws relate to acts of fraud.

(d) Preservation of FTC Authority- Nothing in this Act may be construed in any way to limit or affect the Commission's authority under any provision of law.

(e) Rule of Construction Relating to Required Disclosures to Government Entities- This Act shall not be construed to expand or limit the duty or authority of a covered entity, service provider, or third party to disclose covered information or sensitive information to a government entity under any provision of law.

TITLE VII--MISCELLANEOUS PROVISIONS

SEC. 701. REVIEW.

Not later than 5 years after the effective date of the regulations initially issued under this Act, the Commission shall--

(1) review the implementation of this Act, including the effect of the implementation of this Act on practices relating to the collection, use, and disclosure of covered information and sensitive information; and

(2) prepare and submit to Congress a report on the results of the review under paragraph (1).

SEC. 702. CONSUMER AND BUSINESS EDUCATION CAMPAIGN.

Beginning on the effective date of this Act as set forth in section 703, the Commission shall--

(1) conduct a consumer education campaign to inform individuals of the rights and protections afforded by this Act and the steps that individuals can take to affirmatively consent or decline consent to the collection, use, and disclosure of information under this Act and the regulations issued pursuant to this Act; and

(2) provide guidance to businesses regarding their obligations under this Act, including guidance on how to participate in a Choice Program approved under title IV.

SEC. 703. EFFECTIVE DATE.

This Act shall take effect 2 years after the date of the enactment of this Act. The Commission may stay enforcement of this Act for such period of time as the Commission determines necessary to allow for the establishment and Commission approval of a

Choice Program under title IV and for covered entities to commence participation in such a program.

SEC. 704. SEVERABILITY.

If any provision of this Act, or the application thereof to any person or circumstance, is held unconstitutional or otherwise invalid, the validity of the remainder of the Act and the application of such provision to other persons and circumstances shall not be affected thereby.